REMARKS

Applicant respectfully requests entry of the foregoing amendments and reconsideration of the merits of the outstanding rejections in view of the following remarks. Claims 1-54 are currently pending.

I. Allowable Subject Matter

Applicant notes with appreciation the indication on pages 10 and 11 of the Office Action that claims 5-10, 13, 14, 17-19, 23, 24, 44 and 45 are allowed, and that claims 34 and 35 are allowable if rewritten in independent form. Applicant has opted to defer rewriting claims 34 and 35 in independent form pending reconsideration of the arguments presented below with respect to the rejected independent claims.

II. Overview Of Amendments

The specification has been amended to more accurately describe the present invention. The sentence, "Each application path represents a virtual directory or logical name on a web server representing a physical location of the application(s) on the server(s)," has been rewritten to state: "Each application path is represented as a virtual directory or logical name on a web server representing a physical location of the application(s) on the server(s)." Support for this amendment is found at least at page 10, lines 9-10 and Fig. 2D of the Applicant's Specification.

Independent claims 1 and 27 have been amended to more accurately describe the present invention. More specifically, claims 1 and 27 have been amended to recite "matching an operation request to said application path, wherein said application path is *represented as* a virtual directory or a subdirectory of said application." (emphasis added). Support for these amendments are found at least at page 10, lines 9-10 and Fig. 2D of the Applicant's Specification.

Claims 25, 31, 32 and 36 have been amended to correct typographical errors.

III. The Obviousness Rejection

Claims 1-4, 11, 12, 15, 16, 20-22, 25-33, 36-43, and 46-54 stand rejected under 35 U.S.C. § 103(a), as allegedly unpatentable over "AppShield Provides Block Against Application Hacks," Report on Electronic Commerce, BRP Publications ("BRP") in view of U.S. Patent No. 6,584,569 to Reshef *et al.* ("Reshef"). Office Action at page 2. Particularly, the Examiner contends that BRP teaches all of the claim limitations except for "designating an application path of an application as restricted." *Id.* In an attempt to cure this deficiency, Reshef is introduced as

allegedly disclosing this element. *Id.* The Examiner then opines that "[i]t would have been obvious to one of ordinary skill in the art at the time of the invention to include the application path of the application as restricted with BRP, the motivation is that the detection phase searches for application path parameters in order to check for a vulnerability (see col. 3, lines 60-67)." *Id.*

a. Proposed Combination Would Render AppShield Unsatisfactory For Its Intended Purpose and Would Change Its Principle of Operation

Applicant respectfully submits that the proposed combination is not sufficient to render the claims prima facie obvious because the combination would render AppShield, as disclosed in BRP, unsatisfactory for its intended purpose and would change its principle of operation.

As stated in MPEP § 2143.01, if the proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification. *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Further, if the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959).

i. AppShield Utilizes a Dynamic Security Policy to Prevent Hacking Attempts

BRP vaguely describes an Internet application for security, referred to as "AppShield." *See* BRP, lines 13-14. AppShield implements a dynamic security policy that is generated from examination of the HTML body of every outgoing web page. *See id.* at lines 23-25 ("AppShield recognizes the intended application security policy by analyzing each outbound hypertext markup language (HTML) page"). Any subsequent incoming request is then checked against that dynamic policy. *See id.* at lines 25-26 ("Then it enforces compliance with the policy for each incoming hypertext transfer protocol (HTTP) application"). If a subsequent incoming request is unexpected in view of the dynamic security policy, that request is rejected. *See id.* at lines 30-32 ("AppShield rejects unexpected - and therefore illegal - inputs, generating an error page for the user and notifying the AppShield management log."). AppShield therefore attempts to prevent attacks as they occur through enforcement of the dynamic policy. *See id.* at lines 27-29 ("AppShield protects the integrity of an e-commerce application by making it nearly

impossible for hackers to use traditional security loopholes, either in the applications code or within Web servers.").

ii. Reshef is Directed to Scanning for Application Vulnerabilities

Reshef is directed toward a system for determining web application vulnerabilities. *See* Reshef, abstract. Particularly, Reshef scans for known vulnerabilities by attacking a web application in a simulation mode. *See id.* at col. 2, lines 24-28 ("Then, based on a pre-defined set of hacking rules or techniques, the scanner mutates client requests in various ways, thereby generating exploits that will be unique for each web application. These exploits may then be used to attack the web application.") Reshef then reports the results of the attack to a user so that possible vulnerabilities may be fixed before a real attack occurs. *See id.* at col. 4, lines 27-29 ("The scanner 10 preferably also provides a report 402 recommending fixes or other pertinent advice concerning each detected vulnerability."). Reshef's scanner only identifies vulnerabilities, it does not, by itself, prevent those vulnerabilities from being exploited by hackers.

iii. AppShield and Reshef are Inoperable Together

As discussed above, AppShield operates utilizing a dynamic security policy and attempts to prevent attacks while they occur. This is done by analyzing each outbound hypertext markup language (HTML) page to determine the security policy in place. The functionality of AppShield is premised on the fact that outgoing pages, and in turn the incoming requests for those pages, have met the security policy in place. Thus, unexpected incoming requests are rejected by AppShield. Dissimilarly, Reshef utilizes a scanning mechanism to identify and attack possible vulnerabilities. Combining AppShield with Reshef would result in the attacking mechanism of Reshef bombarding a web application protected by AppShield. In such a situation, AppShield would fail, as the expected incoming requests would in fact be the illegal requests generated by Reshef. Ironically, if Reshef and AppShield were combined, only benign incoming requests would be rejected by AppShield.

Furthermore, AppShield's dynamic policy is generated "on-the-fly" from outgoing web pages, it does not utilize pre-identified information. In contrast, Reshef utilizes a scanning mechanism to merely identify known, and variations of known, vulnerabilities. These vulnerabilities are presented in a static report to the user. Modifying AppShield to utilize previously identified information of known vulnerabilities would not only change its principle of operation, but would also be an unsatisfactory modification of AppShield, as AppShield is

intended to adapt and respond to security vulnerabilities before they can be detected and addressed by traditional means, including the scanner disclosed in Reshef. *See* BRP, lines 17-21.

Combining AppShield with Reshef would result in a security device that rejects only valid incoming requests and does not respond to unknown security vulnerabilities. Furthermore, such a combination would change AppShield's principle of operation of having a dynamic security policy which adapts "on-the-fly.". Accordingly, Applicant respectfully submits that the proposed combination is not sufficient to render the claims obvious and requests the Examiner to withdraw the rejection of claims 1-4, 11, 12, 15, 16, 20-22, 25-33, 36-43, and 46-54

b. The Proposed Combination Does Not Teach or Suggest All of the Claim Limitations

Applicant also respectfully submits that the proposed combination does not teach or suggest all of the limitations recited in the claims. As stated in MPEP § 2143.01, to establish prima facie obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 165 USPQ 494, 496 (CCPA 1970). If an independent claim is nonobvious under 35 U.S.C. 103, then any claim depending therefrom is nonobvious. *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988).

i. Claims 1-4, 11, 12, 15, 16, 20-22, 25 and 26

BRP and Reshef fail to disclose, teach, or suggest each and every element of claims 1-4, 11, 12, 15, 16, 20-22, 25 and 26. More particularly, BRP and Reshef fail to disclose, teach, or suggest at least the following limitations recited in independent claim 1:

> "a method for protecting an application from executing an illegal or harmful operation request received from a distrusted or trusted environment"
>
> and
>
> "designating an application path as restricted"
>
> and
>
> "matching an operation request to said application path"

and

> "determining whether said operation request is illegal or harmful to an environment of said application according to security settings designated for said application path"

The Examiner appears to argue that BRP's disclosure of AppShield, which protects the integrity of an e-commerce application from hackers, discloses, teaches, or suggests the claimed method for protecting an application from executing an illegal or harmful operation request received from a distrusted or trusted environment. See Office Action at page 2. Applicant respectfully disagrees. Neither BRP nor Reshef have any disclosure, teaching, or suggestion regarding protecting an application from executing an operation request from a trusted environment, as claimed in the present application. BRP describes AppShield as an "Internet application" to protect e-commerce sites from hackers. *See* BRP line 13; lines 1-5. Entirely absent from the disclosure in BRP is any suggestion to utilize AppShield on a trusted network or any network aside from the Internet. Similarly, Reshef is only directed towards a scanner to detect security flaws on a web site. *See, e.g.,* Reshef column 1, lines 24-27. Furthermore, Reshef is merely directed to a vulnerability scanner; it identifies vulnerabilities, but does not protect an application from those vulnerabilities. There is no disclosure, teaching, or suggestion in Reshef that third party patches which block certain vulnerabilities are to be applied to applications serving networks other than the Internet. *See* Reshef column 8, lines 36-51. Accordingly, Reshef fails to cure the deficiencies of BRP.

The Examiner acknowledges that BRP does not disclose designating an application path of an application as restricted, but argues that Reshef's disclosure of detecting and identifying potentially vulnerable "application-level messages" discloses, teaches, or suggests the claimed designating an application path of an application as restricted. *See* Office Action at page 2; page 12. Applicant respectfully disagrees. Detecting and identifying a message, as disclosed in Reshef, is distinct from designating an application path. As the present amendments make more clear, an application path is represented as a virtual directory or logical name. *See, e.g,* present application, page 10, lines 7-10. An application path is a physical location of an application on a server. *See, e.g.,* present application page 10, lines 9-10; page 10, line 8; Fig. 2D. It follows that an application path can be represented by a message, but it is not itself a message. An example

makes the distinction clearer: An application path may be represented by more than one virtual subdirectory: "/My App" and "/Your App." In accordance with Reshef, a message containing "/My App" may be detected and identified, but the message containing "/Your App" may not be. In this example, it is clear that Reshef does not disclose detecting and identifying the application path itself, but rather discloses detecting and identifying messages, which, based on chance alone, may represent an application path. Accordingly, Reshef does teach or suggest detecting, identifying, or designating an application path, and cannot designate an application path of an application as restricted, as claimed in the present invention. Thus, Reshef fails to cure the deficiencies of BRP.

The Examiner also appears to argue that recognizing an application security policy by analyzing each outbound hypertext page, and then enforcing compliance with the policy for each incoming page request teaches or suggests the claimed matching an operation request to said application path. *See, e.g.,* Office Action at page 2; page 12. Applicant respectfully disagrees. As discussed above, and fully incorporated herein, an application path is a specific, physical location of an application on a server represented as a virtual directory or logical name. BRP merely discloses protecting an e-commerce application. *See, e.g.,* BRP lines 27-29. As such, it is impossible to know if BRP matches incoming requests to application paths, to a destination server, or something else all together. Indeed, without such minimal disclosure, one cannot know whether BRP conducts any matching at all. BRP may only be relied upon for all that it would reasonably suggest to one having ordinary skill in the art. *See* MPEP § 2128. It is entirely unreasonable to suggest that BRP teaches anything as specific as matching an operation request to an application path, as claimed in the present application. Reshef fails to cure the deficiencies of BRP, as Reshef, as discussed above and fully incorporated herein, identifies messages rather than application paths.

Finally, the Examiner appears to argue that, because AppShield rejects unexpected, illegal inputs, generates an error page for the user, and notifies management of the illegal input, BRP discloses, teaches or suggests the claimed determining whether said application request is illegal or harmful to an environment of said application according to security settings designated from said application path. *See* Office Action at page 2. Applicant respectfully disagrees. BRP does not disclose designating security settings from an application path. The Examiner acknowledges AppShield does not designate an application path as restricted, but also appears to

assert AppShield does designate security settings for an application path. *See id.* Thus, the Examiner appears to make a distinction between an application path having security settings and being restricted. Such a distinction is improper. For an application path to have designated security settings, it must be designated as restricted; an application path without any designated restrictions would have no designated security settings whatsoever. It follows that AppShield cannot teach or suggest determining whether said application request is illegal or harmful to an environment of an application according to security settings designated from said application path, as claimed in the present application. Rehsef does not cure the deficiencies of BRP. Reshef, as discussed above and incorporated herein, has absolutely no teaching or suggestion regarding designating an application path of an application as restricted. Thus, like AppShield, Reshef cannot teach or suggest determining whether an application request is illegal or harmful according to security settings designated from said application path.

Because BRP and Reshef fail to disclose, teach or suggest protecting an application from executing an operation request from a trusted environment, designating an application path of an application as restricted, and determining whether an application request is illegal or harmful according to security settings designated from said application path, Applicant respectfully submits that BRP, either taken alone or in combination with Reshef, fails to teach or suggest all of the limitations recited in independent claim 1 of the present application. Because all the claim limitations are not taught or suggested by the prior art, amended independent claim 1 is nonobvious, and all claims dependent therefrom, *e.g.*, claims 2-4, 11, 12, 15, 16, 20-22, 25 and 26 are also nonobvious.

Although dependent claims 2-4, 11, 12, 15, 16, 20-22, 25 and 26 are allowable at least by virtue of their dependency on independent claim 1, these claims recite additional subject matter which is not suggested by the cited art taken either alone or in combination. For at least the reasons set forth above, Applicant submits that the instant rejection of claims 1-4, 11, 12, 15, 16, 20-22, 25-33, 36-43, and 46-54 is unsustainable, and respectfully requests the Examiner to reconsider and withdraw the obviousness rejection of said claims.

ii. Claims 27-33, 36-43, 46, and 47

Amended claim 27 recites "matching each operation request to an application path, wherein said application path is represented by a virtual directory or a subdirectory of said application; and determining whether each operation request is illegal or harmful to an

environment of said application," which is a similar recitation as found in amended claim 1. Therefore, Applicant respectfully submits that claim 27 is nonobvious at least for the reasons discussed above, and fully incorporated herein, with respect to claim 1.

Although dependent claims 28-33, 36-43, 46, and 47 are allowable at least by virtue of their dependency on independent claim 27, these claims recite additional subject matter which is not suggested by the cited art taken either alone or in combination. For at least the reasons set forth above, Applicant submits that the instant rejection of claims 27-33, 36-43, 46, and 47 is unsustainable, and respectfully requests the Examiner to reconsider and withdraw the obviousness rejection of said claims.

iii. Claims 48-54

BRP and Reshef fail to disclose, teach, or suggest each and every element claims 48-54. More specifically, BRP and Reshef fail to disclose, teach, or suggest at least the following limitations recited in independent claim 48, and similarly recited in claim 51:

> "means for ascertaining an application path of said operation request"
>
> and
>
> "means for embedding said operation request into a data format used by said application"
>
> and
>
> "means for checking a contents of said operation request according to a predefined set of rules associated with said ascertained application path to identify if said operation request is illegal or harmful to an environment of said application"

The Examiner does not appear to identify where either BRP or Reshef disclose, teach, or suggest the claimed means for ascertaining an application path of said operation request. *See* Office Action at page 9. As discussed above, and fully incorporated herein, BRP fails to disclose, teach, or suggest ascertaining an application path of said operation request. The disclosure of BRP is simply too feeble to reasonably teach or suggest anything as specific as ascertaining an application path of said operation request, as claimed in the present application. Reshef fails to

cure the deficiencies of BRP, as Reshef only suggests identifying messages, which is wholly distinct from ascertaining an application path.

The Examiner appears to argue that BRP's disclosure that "AppShield rejects unexpected - and therefore illegal - inputs, generating an error page for the user and notifying the AppShield management log" discloses, teaches or suggests the claimed means for embedding said operation request into a data format used by said application. *See* Office Action at page 9. Applicant respectfully disagrees. BRP does not touch on the subject of embedding operation requests into another data format, particularly one used by an application. Again, BRP may only be relied upon for what it would reasonably suggest to one having ordinary skill in the art. *See* MPEP § 2128. The disclosure cited by the Examiner, and indeed the BRP reference as a whole, fails to reasonably suggest to one skilled in the art embedding an operation request into a data format used by an application, as claimed in the present application. BRP simply fails to provide the specificity needed to render these claims obvious. Reshef does not cure the deficiencies of BRP. Reshef discloses a scanning device that scans for vulnerabilities in an application and then attacks that application. Reshef only discloses receiving an operation request for an application by the application itself; the step of embedding said operation request into a data format used by said application is thus extraneous and entirely outside the teaching of Reshef.

Finally, as discussed above, and fully incorporated herein, BRP and Reshef fail to disclose, teach, or suggest determining whether an operation request is illegal or harmful to an environment of an application according to security settings designated for an application path. It follows that BRP and Reshef also fail to disclose, teach, or suggest variations of that claim, including the claimed means for checking a contents of an operation request according to a predefined set of rules associated with an ascertained application path to identify if said operation request is illegal or harmful to an environment of an application, as recited in independent claim 48, and similarly recited in independent claim 51.

Because BRP and Reshef fail to disclose, teach or suggest ascertaining an application path of said operation request, means for embedding said operation request into a data format used by said application, and means for checking a contents of said operation request according to a predefined set of rules associated with said ascertained application path to identify if said operation request is illegal or harmful to an environment of said application, Applicant respectfully submits that BRP, either taken alone or in combination with Reshef, fails to teach or

suggest all of the limitations recited in independent claim 48, and similarly recited in independent claim 51, of the present application. Because all the claim limitations are not taught or suggested by the prior art, independent claims 48 and 51 are nonobvious, and all claims dependent therefrom, *e.g.*, claims 49, 50 and 52-54 are also nonobvious.

Dependent claims 49, 50, and 52-54 are allowable at least by virtue of their dependency on independent claims 48 and 51. For at least the reasons set forth above, Applicant submits that the instant rejection of claims 48-54 is unsustainable, and respectfully requests the Examiner to reconsider and withdraw the obviousness rejection of said claims.

IV. Conclusion

In view of the foregoing, it is respectfully submitted that the present application is in condition for allowance, and an early indication of the same is courteously solicited. The Examiner is respectfully requested to contact the undersigned by telephone at the below listed telephone number, in order to expedite resolution of any issues and to expedite passage of the present application to issue, if any comments, questions, or suggestions arise in connection with the present application.

Applicant is submitting herewith a Petition for a Three-Month Extension of time, along with the requisite fees. In the event that the U.S. Patent and Trademark Office requires additional fees to enter and/or consider this Reply, or to prevent abandonment of the present application, please charge such fees to the undersigned's Deposit Account No. 50-2613, Order No. 58525.00004.UTL1.P1068).

Respectfully submitted,

Dated: June 15, 2006 By: _____

Todd M. Schneider, Patent Agent
Registration No. 57,629
for Trevor Q. Coddington, Ph.D., Esq.
Registration No. 46,633

PAUL, HASTINGS, JANOFSKY & WALKER LLP
Customer Number: 36183
P.O. Box 919092
San Diego, CA 92191-9092
Telephone: (858) 720-2500
Facsimile: (858) 720-2555